(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95558 A1

(51) International Patent Classification[7]: H04L 9/14

(21) International Application Number: PCT/US01/18127

(22) International Filing Date: 5 June 2001 (05.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/587,603 5 June 2000 (05.06.2000) US

(71) Applicant: MATSUSHITA MOBILE COMMUNICATION DEVELOPMENT CORPORATION OF U.S.A. [US/US]; Suite 2-407, 1225 Northbrook Parkway, Suwanee, GA 30024 (US).

(72) Inventor: FORDER, David; 3380 Duncan Bridge Road, Buford, GA 30519 (US).

(74) Agent: SMITH, Gregory, Scott; Troutman Sanders LLP, Bank of America Plaza, Suite 5200, 600 Peachtree Street, N.E., Atlanta, GA 30308-2216 (US).

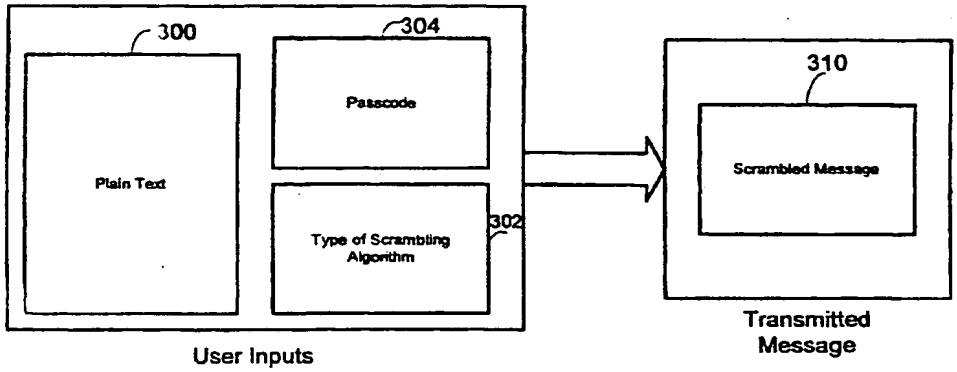
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTOCOL FOR SHORT MAIL MESSAGE ENCRYPTION



(57) Abstract: A method to provide privacy and security for Short Mail (SMS) messages (300) by invoking integrated algorithms to provide additional scrambling of the SMS text based on a passcode (304) entered by the sender into a cellular or PCS device. The device will send character strings that are valid within the existing acceptable character limitations of the SMS protocol. The transmitted scrambled message (310) will include a header that indicates the type of scrambling algorithm (302) used, but not the passcode (304). The remote receiver device will receive the scrambled message (310) and recognize that is scrambled by the encryption header located at the beginning of the text portion of the message. When the remote user receives the message, the device will prompt the user for a passcode (304). If the correct passcode (304) is entered, the device will execute a complimentary decoding algorithm using the entered passcode (304) as a key. The original unscrambled message will then be displsayed as a plain text (300). If an incorrect passcode (304) is entered, the device will not display the original unscrambled message in plain text (300). If the scrambled message (310) is sent to a device that does not support unscrambling, the message will appear as garbage text.

WO 01/95558 A1

PROTOCOL FOR SHORT MAIL MESSAGE ENCRYPTION

FIELD OF INVENTION

This invention relates generally to radio communication networks that use digital control channel access methods and, more specifically, Time Division Multiple Access (TDMA) and Global System for Mobile communication (GSM) networks that are capable of supporting Short Message Service (SMS) messaging. This invention also relates to SMS message encryption.

BACKGROUND OF THE INVENTION

Cellular, PCS and GSM networks of radio telephones and pagers continue to grow in popularity as they become more affordable and accessible for new customers. These systems operate using digital protocols that maximize flexibility by allowing mobility and choice of communication. Voice, text and Internet communications are supported by many of these systems over vast coverage areas. As a result, mobile devices are increasingly being used as the primary communications medium for personal and business relations.

Short Message Service (SMS) messaging is a popular wireless messaging standard. SMS messages can be used to transmit a variety of information such as system status reports and other

practical information such as weather reports, news and traffic updates. Unlike paging systems, the SMS protocol does not require a transmitting unit to be within a service area for a message to be sent successfully. An SMS message can be stored, potentially for days, to be sent when the unit returns to a service area. SMS messages can be transmitted from base stations to a plurality of mobile units or from one mobile unit to another. Therefore, the SMS protocol can be used to convey personal messages between mobile users.

A drawback of current digital wireless networks is that these systems must ration the radio spectrum between various users. Network designers have been challenged to devise methods to handle increasing wireless traffic. Methods to manage growth in capacity have to be weighed in relation to acceptable consumer quality tolerance levels. Examples of current commercially deployed digital wireless systems are GSM, TDMA and Code Division Multiple Access (CDMA). Future wireless networks will build on these technologies to employ common worldwide standards for seamless movement between systems across the globe.

Current commercial networks are differentiated by the methods they employ to accommodate multiple users on a single radio control channel. A feature of multiple access methods like TDMA and CDMA is that for a particular conversation or message stream, network users will share multiple control channels with multiple users. Therefore, it is possible for outsiders to access a private conversation or message as a result of shared channel access methods.

A method has been devised for digital control channels having logical channels to support broadcast SMS messages. Information sent from a base station to a remote station such as

broadcast control information can be encoded according to an error correcting code and include a plurality of bits with inverse polarities of cyclic redundancy check (CRC) bits produced by the encoding. An example of this method is described in U.S. Pat. No. 5,768,276 to Diachina et al. One disadvantage of this method is that although the method is capable of broadcasting encrypted SMS messages to accommodate extra cost consumer services similar to premium cable television service, it does not address private, non-broadcast communication security.

Therefore, there is a need in the art for a method to provide additional privacy and security for the sensitive text contained in traditional Short Mail (SMS) messages used for private communication between mobile users.

SUMMARY OF THE INVENTION

The present invention overcomes the above-described problems in the prior art by providing a method for SMS message encryption between mobile stations that enhances privacy and security for the transmission of personal messages.

The present invention overcomes the problems of the prior art by providing a cellular, PCS or GSM mobile station that can invoke integrated algorithms that scramble message text. These scrambling algorithms can be of any number of protocols used for scrambling text like those currently used in the art.

Generally described, the present invention provides a method for transmitting scrambled SMS messages using a passcode key. The transmitted messages can be unscrambled by the remote user with the corresponding unscrambling passcode. When a invalid

passcode is entered by the remote user the message will not be unscrambled.

The integrated algorithms will utilize a passcode key system to scramble message text. The passcode may either utilize a public key system where the receiver can obtain the decrypting passcode or a private key system that would be exchanged only between the sender and the proper receiver. The user interface of the mobile station will prompt the transmitting user (the sender of the message) to enter a passcode. The invention will allow for the characters that are sent, even after being encrypted, to still be valid within the acceptable character string limitations of the SMS protocol.

One embodiment of the present invention provides for the transmitted message to include a header that will indicate the type of encoding method used, the senders text message and other control and error correcting information, but not the passcode needed to decrypt the message. The remote receiver device (mobile receiving unit) will receive the encoded message and recognize that it contains scrambled text from the "scrambling header" that will be located at the beginning of the text portion of the message character string.

In another embodiment of the present invention, the transmitted message does not include in the header an indication that the message is encrypted. In this embodiment, either the encrypted text can be displayed or, an encryption detector within the receiving device can parse the received message to determine if it is encrypted. The invention provides for the display of the receiving device to indicate that the message received contains scrambled text. The message will be stored until the remote user wishes to read the text by a method well known in the art by one of ordinary skill and as

implemented in many devices such as radio telephones that have text messaging capabilities.

When the receiving user wishes to read the message, the user interface of the remote device will prompt the user for a passcode to implement a complimentary decoding algorithm appropriate for the encoding method utilized by the sender. If the passcode entered by the remote user is correct, then the unscrambled message text will be displayed by the mobile receiving unit. If an incorrect passcode is entered, garbage text will be displayed.

In one embodiment of the present invention, if the user enters an invalid passcode, the user interface will display an error statement and prompt the user to enter the correct passcode.

In another embodiment of the present invention, the mobile receiving unit is preprogrammed to allow a certain number of invalid passcode entries before erasing the text message from the device's memory.

In another embodiment of the present invention, the mobile receiving unit is preprogrammed to allow a certain number of invalid passcode entries by the receiving user before returning a message to the sender that the remote user did not enter a valid passcode to read the encoded message.

Objects, features and advantages of the present invention will become apparent upon reading the following detailed description of the preferred embodiments of the invention, when taken in conjunction with the accompanying drawings and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a system diagram that illustrates an exemplary environment suitable for implementing various embodiments of the present invention.

Fig. 2 is a block diagram of an exemplary environment suitable to provide mobile to mobile SMS message communication.

Fig. 3 is a block diagram illustrating the components of a scrambled SMS message.

Fig. 4 shows the partitioning of data in an SMS message frame structure.

Figs. 5A-5B shows the partitioning of text data in a scrambled SMS message.

Fig. 6 is a flow chart illustrating the steps of an exemplary embodiment of the present invention.

Fig. 7 is a flow chart illustrating the steps of an exemplary embodiment of the present invention.

DETAILED DESCRIPTION

Referring now in detail to the drawings in which like numerals refer to like parts throughout the several views. Fig. 1 is a system diagram that illustrates an exemplary environment suitable for implementing various embodiments of the present invention. Fig. 1 and the following discussion provide a general overview of a platform onto which the invention may be integrated or implemented. Although in the context of the exemplary environment the invention will be described as consisting of instructions within a software program being executed by a processing unit, those skilled in the art will understand that portions of the invention, or the entire invention

itself may also be implemented by using hardware components, state machines, or a combination of any of these techniques. In addition, a software program implementing an embodiment of the invention may run as a stand-alone program or as a software module, routine, or function call, operating in conjunction with an operating system, another program, system call, interrupt routine, library routine, or the like. The term "program module" will be used to refer to software programs, routines, functions, macros, data, data structures, or any set of machine readable instructions or object code, or software instructions that can be compiled into such, and executed by a processing unit.

Those skilled in the art will appreciate that the system illustrated in Fig. 1 may take on many forms and may be directed towards performing a variety of functions. Examples of such forms and functions include cellular telephones, radio telephones, portable telephones, two-way pagers, personal computers, hand-held devices such a personal data assistants and calculators, consumer electronics, note-book computers, lap-top computers, and a variety of other applications, each of which may serve as an exemplary environment for embodiments of the present invention.

The exemplary system illustrated in Fig. 1 includes a computing device **110** that is made up of various components including, but not limited to a processing unit **112**, non-volatile memory **114**, volatile memory **116**, and a system bus **118** that couples the non-volatile memory **114** and volatile memory **116** to the processing unit **112**. The non-volatile memory **114** may include a variety of memory types including, but not limited to, read only memory (ROM), electronically erasable read only memory (EEROM),

electronically erasable and programmable read only memory (EEPROM), electronically programmable read only memory (EPROM), electronically alterable read only memory (EAROM), FLASH memory, bubble memory, and battery backed random access memory (RAM). The non-volatile memory **114** provides storage for power on and reset routines (bootstrap routines) that are invoked upon applying power or resetting the computing device **110**. In some configurations the non-volatile memory **114** provides the basic input/output system (BIOS) routines that are utilized to perform the transfer of information between elements within the various components of the computing device **110**.

The volatile memory **116** may include, but is not limited to, a variety of memory types and devices including, but not limited to, random access memory (RAM), dynamic random access memory (DRAM), FLASH memory, EEPROM, bubble memory, registers, or the like. The volatile memory **116** provides temporary storage for routines, modules, functions, macros, data etc. that are being or may be executed by, or are being accessed or modified by the processing unit **112**. In general, the distinction between non-volatile memory **114** and volatile memory **116** is that when power is removed from the computing device **110** and then reapplied, the contents of the non-volatile memory **114** remain intact, whereas the contents of the volatile memory **116** are lost, corrupted, or erased.

The computing device **110** may access one or more external display devices **130** such as a CRT monitor, LCD panel, LED panel, electro-luminescent panel, or other display device, for the purpose of providing information or computing results to a user. In some embodiments, the external display device **130** may actually be

incorporated into the product itself. The processing unit **112** interfaces to each display device **130** through a video interface **120** coupled to the processing unit **110** over the system bus **118**.

The computing device **110** may send output information, in addition to the display **130**, to one or more output devices **132** such as a speaker, modem, printer, plotter, facsimile machine, RF or infrared transmitter, computer or any other of a variety of devices that can be controlled by the computing device **110**. The processing unit **112** interfaces to each output device **132** through an output interface **122** coupled to the processing unit **112** over the system bus **118**. The output interface may include one or more of a variety of interfaces, including but not limited to, an RS-232 serial port interface or other serial port interface, a parallel port interface, a universal serial bus (USB), an optical interface such as infrared or IRDA, an RF or wireless interface such as Bluetooth, or other interface.

The computing device **110** may receive input or commands from one or more input devices **134** such as a keyboard, pointing device, mouse, modem, RF or infrared receiver, microphone, joystick, track ball, light pen, game pad, scanner, camera, computer or the like. The processing unit **112** interfaces to each input device **134** through an input interface **124** coupled to the processing unit **112** over the system bus **118**. The input interface may include one or more of a variety of interfaces, including but not limited to, an RS-232 serial port interface or other serial port interface, a parallel port interface, a universal serial bus (USB), an optical interface such as infrared or IrDA, an RF or wireless interface such as Bluetooth, or other interface.

It will be appreciated that program modules implementing various embodiments of the present invention may be may be stored in the non-volatile memory **114**, the volatile memory **116**, or in a remote memory storage device accessible through the output interface **122** and the input interface **124**. The program modules may include an operating system, application programs, other program modules, and program data. The processing unit **112** may access various portions of the program modules in response to the various instructions contained therein, as well as under the direction of events occurring or being received over the input interface **124**.

The computing device **110** may transmit signals to, or receive signals from, one or more communications systems **136** such as a cellular network, RF network, computer network, cable network, optical network or the like. The processing unit **112** interfaces to each communications system **136** through a transmitter **126** and a receiver **128**, both coupled to the processing unit **112** over the system bus **118**. The transmitter **126** and the receiver **128** may include one or more of a variety of transmission techniques such as a radio frequency interface (AM, FM, PSK, QPSK, TDMA, CDMA, Bluetooth or other technique) or an optical interface such as infrared or IrDA.

Fig. 2 is a block diagram of an exemplary environment suitable to provide mobile to mobile SMS message communication. A mobile transmitting unit **200** contains an output device in the form of a voice and control channel transceiver **126**, a processing unit **112**, a memory device **116**, input **134** and output **132** user interface and a power source (not shown). When a user wishes to send a SMS message to another user, the message is transmitted through a

communications system **136** and relayed on to the receiving unit **210**. The receiving unit **210** also has an input device in the form of a voice and control channel transceiver **128**, a processing unit **212**, a memory device **216**, an input **234** and output **232** user interface and a power source (not shown). Although the present invention is described in conjunction with cellular communication media, those skilled in the art will understand that the present invention need not be so limited, and could find uses in communications systems of other types such as an SMS gateway website. In addition, SMS messaging could also occur through satellite transmitting and receiving devices or over two-way telephone or data transmission systems.

In the general operation of an exemplary embodiment of the present invention, the processing unit **112** of the mobile transmitting unit **200** receives an inputted SMS message from the user interface **134**. A passcode is entered through the user interface **134** directing the processing unit **112** to scramble the entered message. The message is directed by the processing unit **112** to be scrambled by an integrated scrambling algorithm stored in and read from the memory **116**.

The identifier of the recipient, which could be a telephone number, email address, or other identification protocol, is entered through the user interface **134** to send the scrambled message to a particular receiver. The voice and control channel transceiver **126** is then used to transmit the scrambled SMS message to a particular address.

In a typical cellular telephone communications system **136**, a base station within a geographic area defines the service area. For this particular invention, the base station receives radio frequency

(RF) signals from the transmitting mobile unit **200** and sends RF signals to the mobile receiving unit **210**.

The mobile receiving unit **210** receives the RF signals from the communications system **136** with the voice and control channel transceiver **128**. The received SMS message will be saved in memory **216**. The passcode entered through the user interface **234** directs the processing unit **212** to unscramble the received scrambled message. The unscrambled message will be displayed through an output device **232**.

Fig. 3 is a block diagram illustrating the components of a scrambled SMS message. Using this invention, an SMS message will be constructed by user inputs of plain text **300**, a passcode **304**, and a selection of an integrated scrambling algorithm **302**. The plain text **300** of the SMS message can be inputted through a user interface **134** or can be recalled from memory **116**. The input user interface **134** could be a keypad or another text entry method (or a combination of text entry methods) well understood by those skilled in the art. The selection of the integrated scrambling algorithm **302** can be entered through the user interface **134** or may be defaulted. In certain embodiments, only a single algorithm may be used.

The present invention could utilize encryption techniques such as Pretty Good Privacy (PGP) or others well understood by those skilled in the art. Alternatively, scrambling algorithms could be downloaded by the mobile transmitting unit **200** from external sources. As will be seen below, the type of scrambling algorithm used can be encoded in the scrambled message **310** that is transmitted.

A public or private key passcode **304** can be inputted through the user interface **134** to be used as a key for scrambling an

SMS message with the selected integrated scrambling algorithm to create the scrambled message **310** that will be transmitted to the mobile receiving unit **210**. The passcode could be any combination of alphanumeric characters and could be of any length. In an alternative embodiment, a user can prestore scrambling passcodes **304** based on recipient addresses. SMS messages sent to recipients with prestored scrambling passcodes **304** will be scrambled using the integrated scrambling algorithm corresponding to the assigned scrambling passcode **304** without requiring further user inputs. As will be seen below, the passcode **304** will not be encoded in the scrambled message **310** that is transmitted.

Fig. 4 shows the partitioning of data in an SMS message frame structure **400**. An SMS message frame **400** can be divided into two major parts. The text **420** of the SMS message contains the alphanumeric characters of the SMS message being sent. The SMS header **410** contains the functional information necessary for sending and receiving an SMS message. In one embodiment, the header may contain the type of scrambling algorithm used to scramble the SMS message, routing information, length of the message text **420**, character type (e.g. ASCII, ISO) used in the text message **420**, and error correction bits among other information, well understood by those of ordinary skill in the art, that would be included in an SMS header **410**.

Fig. 5A shows the partitioning of text data in a scrambled SMS message. A block at the beginning of the message frame **400** contains the SMS header **410**, characters indicating the encryption type **502** used to scramble the SMS message. This block is followed by the actual scrambled characters of the SMS message. In this

embodiment, the processing unit **112** detects when an entered passcode is not correct by utilizing a checksum **504** based on the plain text **300** of the SMS message. A checksum **504** can be added to the SMS message frame **400** by methods well known to those of ordinary skill in the art.

Fig. 5B shows the partitioning of text data in a scrambled SMS message. In this embodiment, the processing unit **112** detects when an entered passcode is not correct by utilizing a CRC method **506** based on the plain text **300** of the SMS message. A CRC polynomial can be added to the SMS message frame **400** by methods well known to those of ordinary skill in the art.

Fig. 6 is a flow chart illustrating the steps of an exemplary embodiment of the present invention. To transmit a scrambled SMS message a user utilizing the present invention will first compose the written text message **600**. The user will then choose a scrambling method **602** either from a selection of integrated scrambling algorithms contained within the memory **116** of the mobile transmitting unit **200** or could download a scrambling algorithm from an external source. In an alternate embodiment utilizing a single algorithm, the step **602** can be eliminated. The user will then enter an alphanumeric passcode **604** to be used as the key to scramble and unscramble the SMS message. In an alternate embodiment, the user may be prompted to enter the passcode. The passcode can be of any length and could be derived from a public or private key encryption system. Upon the user's input of the passcode **604**, the processing unit **112** will utilize the integrated scrambling algorithm stored in memory **116** to scramble the SMS message **606**. The user can then direct the processing unit **112** (through the user

interface input device **134**) to send the scrambled SMS message **608** by utilizing the voice and control channel transceiver **132.**

Fig. 7 is a flow chart illustrating the steps of an exemplary embodiment of the present invention. When the mobile receiving unit **210** receives a scrambled SMS message with its voice and control channel transceiver **128**, the scrambled SMS message **310** will be saved **700** in the memory **116**. The receiving user would be prompted with the choice of whether to read the scrambled SMS message **310** now or whether they would rather save the message to be read later **702**. This choice might be presented to the receiving user through the user interface **134** with a message that could read "PRESS OK TO READ NEW MESSAGE, PRESS "1" TO SAVE". If the user chooses not to read the message at the present time, the message will be stored for future access, depending on the type of mobile receiving unit, by methods that are well understood by those of ordinary skill in the art. If the user chooses to read the message presently, the user will be prompted through the user interface **132** to enter a passcode **704**. The user will use the user interface **134**, which could be an alphanumeric keypad, to enter a passcode. The processing unit **112** will compare the entered passcode with the passcode necessary to unscramble the scrambled SMS message **706**. If the passcode is not the correct passcode to unscramble the SMS message then the user will be prompted through the user interface **118** to enter the correct passcode again **704**. In an ideal embodiment of the present invention, the user could be given a predetermined number of chances to enter the correct passcode. If the user does not enter the correct passcode after the predetermined number of chances, the mobile receiving unit **210** will transmit a message utilizing the voice

and control channel transceiver back to the sender of the scrambled SMS message **310** informing the transmitting user that the scrambled SMS message **310** was not successfully unscrambled by the receiving user. Such a message could read "MESSAGE ERROR. RECIPIENT COULD NOT OPEN." The transmitting user could then either terminate efforts to send the SMS message or send the SMS message again. In another ideal embodiment, the processing unit **112** will attempt to unscramble the SMS message when a passcode **304** is entered based on the corresponding integrated descrambling algorithm. If the passcode **304** is not correct, the display **130** will show garbage text.

If the receiving user enters the correct passcode, the processing unit **112** will unscramble the SMS message utilizing the complementary integrated unscrambling algorithm from the memory **116**. Alternatively, the complementary unscrambling algorithm could be downloaded by the mobile receiving unit **210** from an external source.

While this invention has been described in detail with particular reference to preferred embodiments thereof, it will be understood that variations and modifications can be effected within the scope of the invention as defined in the appended claims.

CLAIMS

What is claimed is:

1. A method for providing privacy for SMS messages exchanged between a first device and a second device without requiring the use of system components to provide such privacy, the method comprising the steps of:

providing an SMS message to the first device;

providing a passcode to the first device;

invoking an integrated scrambling algorithm within the first device with the passcode to scramble the SMS message;

transmitting the scrambled SMS message to the second device;

receiving the scrambled SMS message at a second device;

providing the passcode to the second device independent from any system components; and

invoking an integrated unscrambling algorithm within the second device with the passcode to recover the SMS message.

2. Method of claim 1, wherein the step of invoking an integrated scrambling algorithm within the first device comprises the step of selecting one of a plurality of integrated scrambling algorithms;

3. Method of claim 2, wherein a header is added to the scrambled SMS message to indicate which integrated scrambling algorithm of the plurality of integrated scrambling algorithms was used to scramble the SMS message;

4. Method of claim 2, wherein a header is added to the scrambled SMS message to indicate that an integrated scrambling algorithm was used to scramble the SMS message.

5. Method of claim 1, wherein the step of invoking an integrated unscrambling algorithm within the second device comprises the step of selecting one of a plurality of integrated unscrambling algorithms.

6. Method of claim 1, wherein the scrambled SMS message is transmitted within SMS character string limitations.

7. Method of claim 1, wherein a plurality of passcodes can be used to select a plurality of integrated scrambling algorithms.

8. Method of claim 1, wherein a passcode is automatically selected based on the identity of the receiver.

9. Method of claim 1, wherein the passcode is pre-stored in the first device.

10. Method of claim 1, wherein the receiver is prompted to enter the passcode into the second device.

11. Method of claim 1, wherein if the passcode does not correspond to the passcode corresponding to the integrated scrambling algorithm, an error message is displayed.

12. Method of claim 1, wherein if the passcode does not correspond to the passcode corresponding to the integrated scrambling algorithm, the scrambled SMS message is displayed.

13. Method of claim 1, wherein if the passcode does not correspond to the passcode corresponding to the integrated scrambling algorithm, a readout error message is sent back to the transmitter of the scrambled SMS message.

14. A first device comprising of:

a controller;

a user-selected passcode;

a transmitter coupled to the controller;

a memory device coupled to the controller and containing an integrated scrambling algorithm;

the controller, using the user-selected passcode to select the integrated scrambling algorithm contained in the memory device, being operative to scramble an SMS message;

the transmitter, being coupled to the controller, being operative to transmit the scrambled SMS message.

15. The device of claim 14, wherein the transmitter is operative to transmit the scrambled SMS message within SMS character string limitations.

16. The device of claim 14, wherein a plurality of user-selected passcodes can be used to select a plurality of integrated scrambling algorithms.

17. The device of claim 14, wherein the user-selected passcode is automatically selected based on the identity of the receiver.

18. The device of claim 14, wherein the user-selected passcode is pre-stored.

19. A second device comprising of:

a controller;

a user-selected passcode;

a receiver coupled to the controller;

a memory device coupled to the controller and containing an integrated unscrambling algorithm;

the receiver, being operative to receive a scrambled SMS message;

the controller, being coupled to the receiver and using the user-selected passcode to select the integrated unscrambling algorithm contained in the memory device, being operative to unscramble the scrambled SMS message;

20. The device of claim 19, wherein the receiver is prompted to enter the user-selected passcode.

21. The device of claim 19, wherein if the user-selected passcode does not correspond to the user-selected passcode corresponding to the integrated scrambling algorithm, an error message is displayed.

22. The device of claim 19, wherein if the user-selected passcode does not correspond to the user-selected passcode corresponding to the integrated scrambling algorithm, the scrambled SMS message is displayed.

23. The device of claim 19, wherein if the user-selected passcode does not correspond to the user-selected passcode corresponding to the integrated scrambling algorithm, a readout error message is sent back to the transmitter of the scrambled SMS message.

24. A system for providing privacy for SMS messages comprising of:

a first device;

a second device;

a communication system;

the controller of the first device, using the user-selected passcode to select the integrated scrambling algorithm

contained in the memory device, being operative to scramble an SMS message;

the transmitter of the first device, being coupled to the controller, being operative to transmit the scrambled SMS message through the communications system;

the receiver of the second device being operative to receive the scrambled SMS message through the communications system;

the controller of the second device, being coupled to the receiver and using the user-selected passcode to select the integrated scrambling algorithm contained in the memory device, being operative to unscramble the scrambled SMS message.

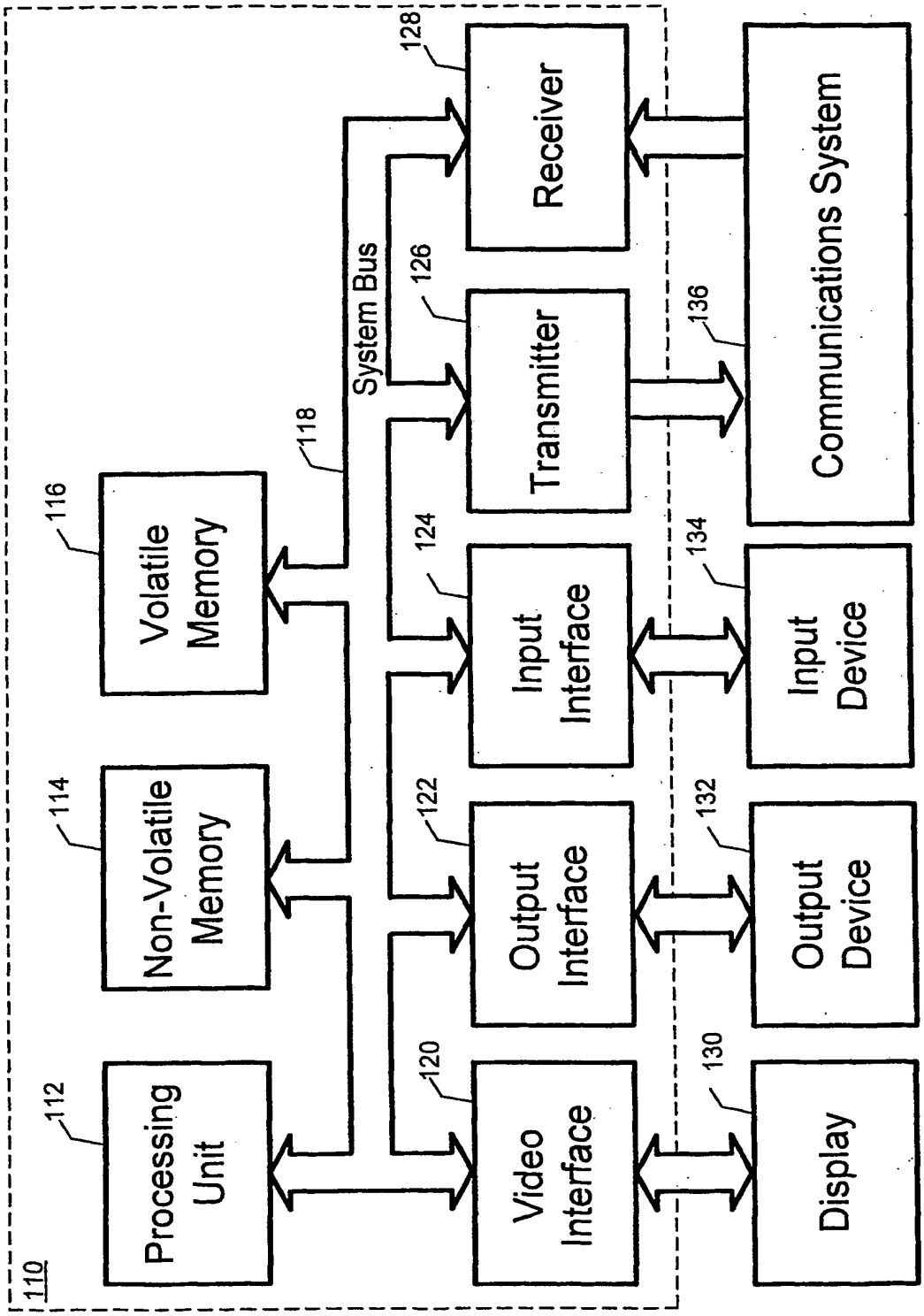

110
Processing Unit
112
Non-Volatile Memory
114
Volatile Memory
116
118
System Bus
Video Interface
120
Output Interface
122
Input Interface
124
Transmitter
126
Receiver
128
Display
130
Output Device
132
Input Device
134
136
Communications System

Fig. 1

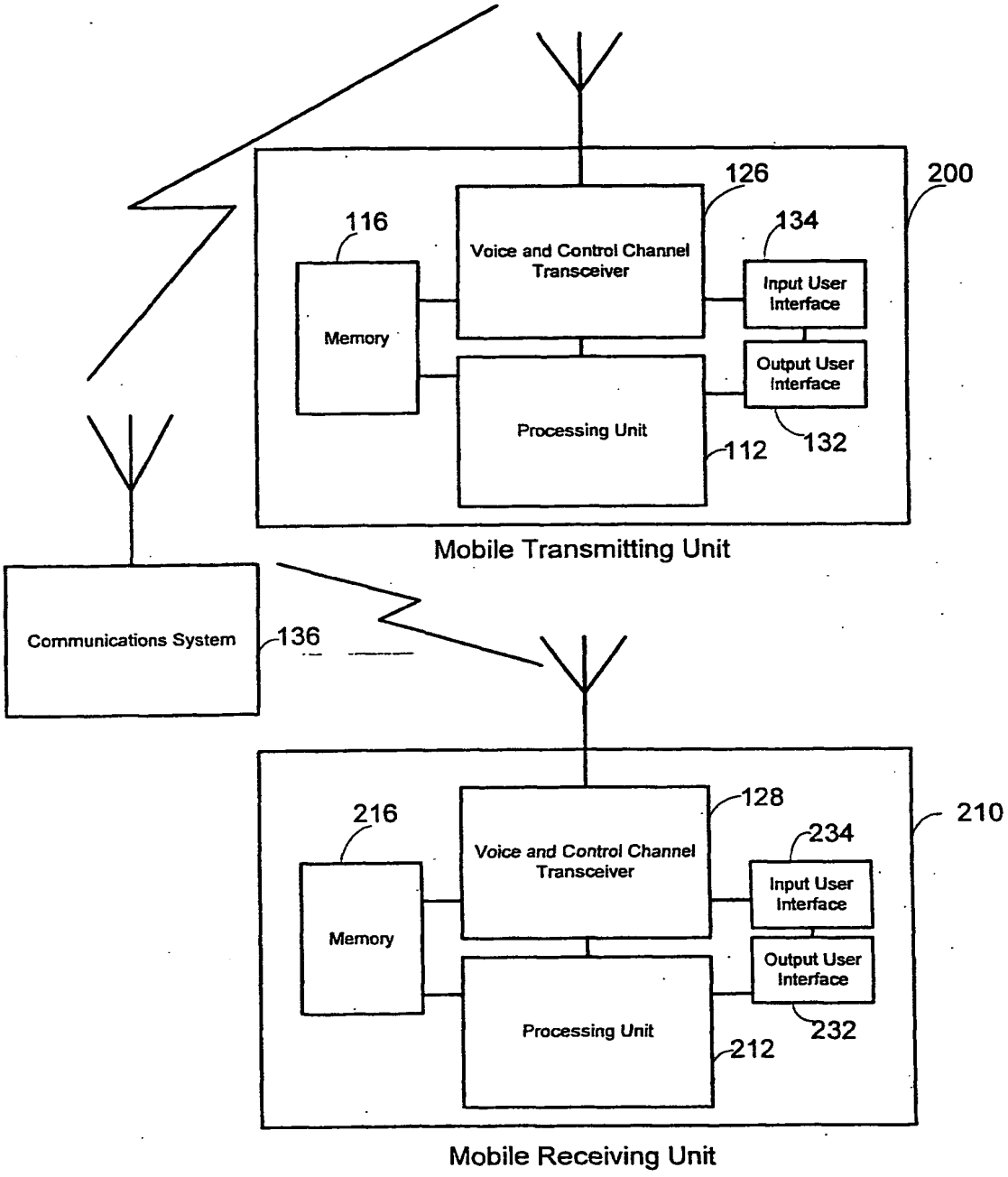

126
200
116
134
Voice and Control Channel Transceiver
Input User Interface
Memory
Output User Interface
Processing Unit
112
132
Mobile Transmitting Unit
Communications System
136
128
210
216
234
Voice and Control Channel Transceiver
Input User Interface
Memory
Output User Interface
Processing Unit
232
212
Mobile Receiving Unit

Fig. 2

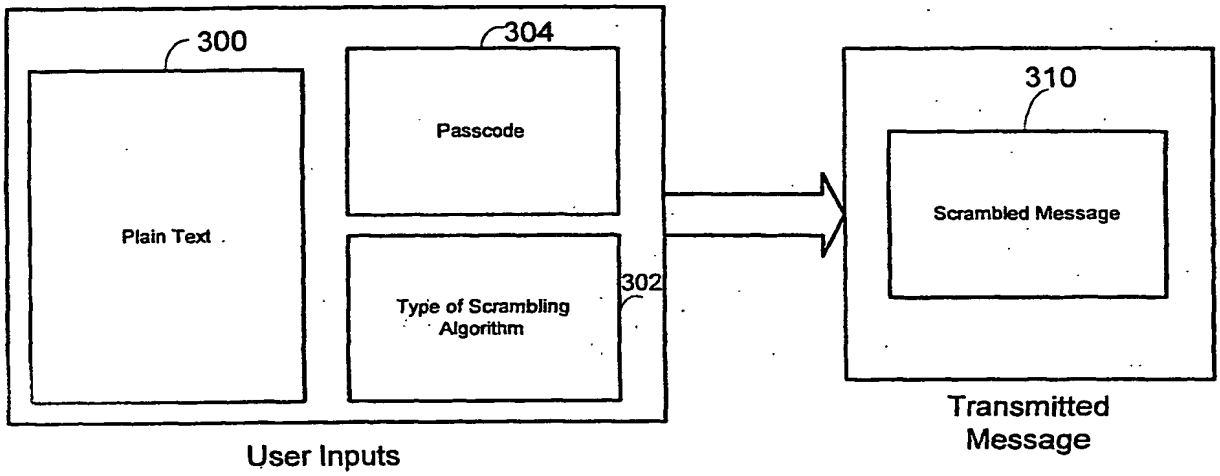
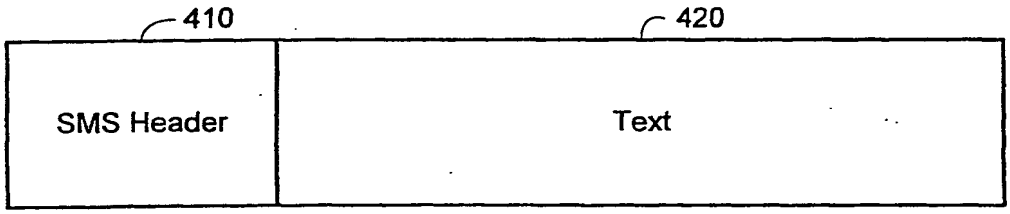

300
304
Passcode
Plain Text
Type of Scrambling Algorithm
302
User Inputs
310
Scrambled Message
Transmitted Message

Fig. 3



SMS Message Frame
400

Fig. 4

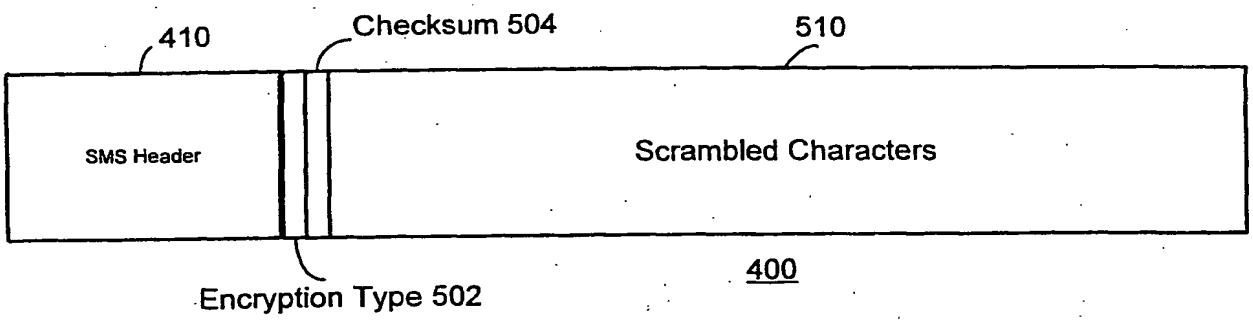

410
Checksum 504
510
SMS Header
Scrambled Characters
400
Encryption Type 502

Fig. 5A

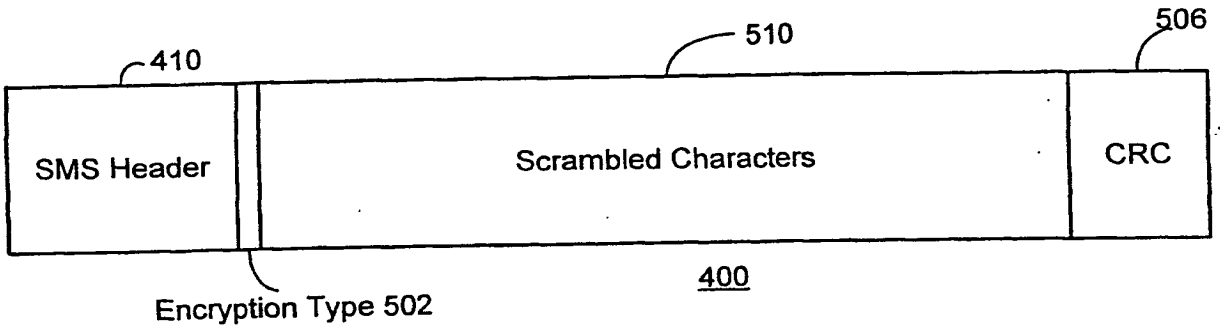

410
510
506
SMS Header
Scrambled Characters
CRC
400
Encryption Type 502

Fig. 5B

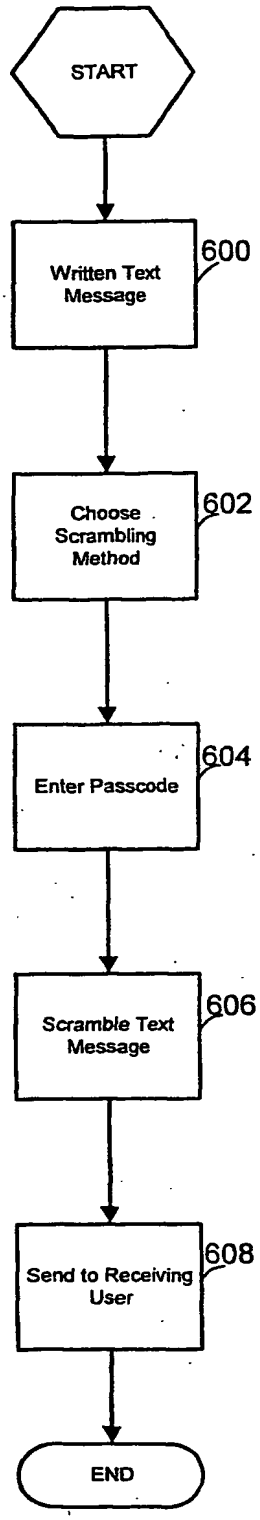

START
Written Text Message
600
Choose Scrambling Method
602
Enter Passcode
604
Scramble Text Message
606
Send to Receiving User
608
END

Fig. 6

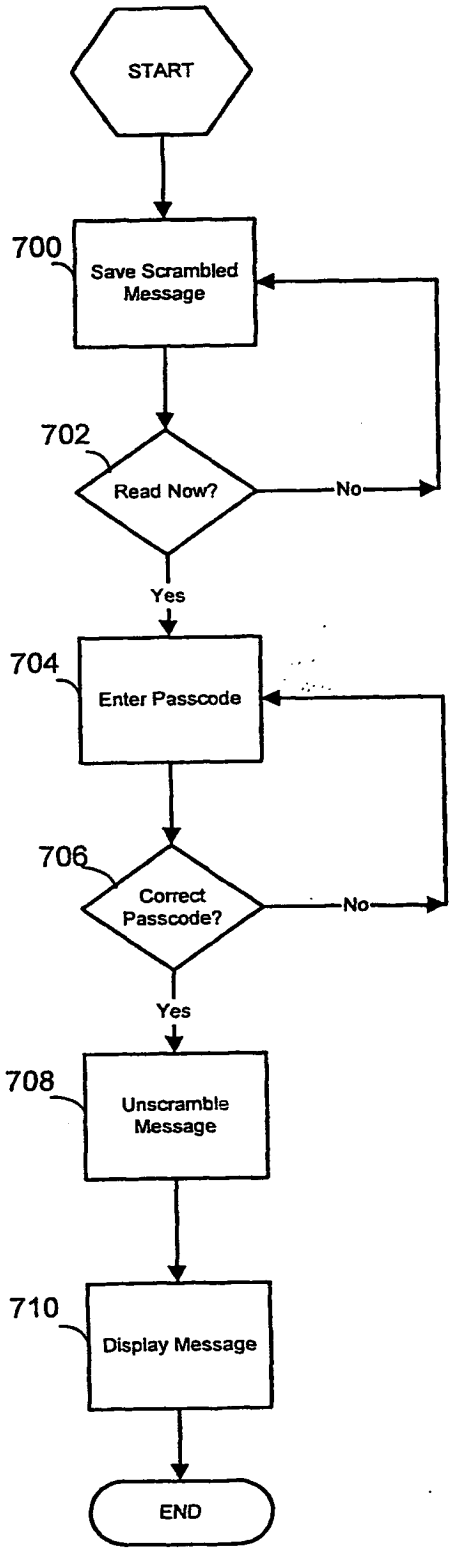

START
700
Save Scrambled Message
702
Read Now?
No
Yes
704
Enter Passcode
706
Correct Passcode?
No
Yes
708
Unscramble Message
710
Display Message
END

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/18127

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/14
US CL : 380/259
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/259, 268, 270, 42, 43; 713/160, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS via EAST
search terms: encrypt, scramble, encode, short, SMS, text, message, password, passcode, passphrase

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 6,125,281 A (WELLS et al.) 26 September 2000, column 3, line 55 through column 4, line 10.	1-24
Y	US 5,768,276 A (DIACHINA et al.) 16 June 1998, column 23, lines 9-42.	1-24
Y	US 5,787,172 A (ARNOLD) 28 July 1998, column 35, line 49.	3 and 4
Y	US 5,737,422 A (BILLINGS) 07 April 1998, column 3, lines 7-20	1-24
Y	US 5,953,424 A (VOGELESANG et al.) 14 September 1999, column 3, lines 46-57.	1-24
Y	US 5,988,510 A (TUTTLE et al.) 23 November 1999, column 4, lines 34-54.	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 AUGUST 2001	Date of mailing of the international search report 18 OCT 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Gail Hayes Telephone No. (703) 306-5617

Form PCT/ISA/210 (second sheet) (July 1998)*

THIS PAGE BLANK (USPTO)